



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,224	09/12/2003	Partha Bhattacharya	50325-1085	6837
29989 7590 08/09/2007 HICKMAN PALERMO TRUONG & BECKER, LLP 2055 GATEWAY PLACE SUITE 550 SAN JOSE, CA 95110			EXAMINER TRAN, MYLINH T	
			ART UNIT 2179	PAPER NUMBER
			MAIL DATE 08/09/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/661,224	BHATTACHARYA ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Mylinh Tran	2179	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 25 April 2007.
- 2a) ☐ This action is **FINAL**.
- 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) 8-15 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-7 and 16-31 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All    b) ☐ Some \*    c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Election/Restrictions***

Applicant has elected for prosecution group I, without traverse. Election was made **without** traverse in the reply filed on 04/25/07. The restriction is hereby made final.

### ***Specification***

Claims 25-31 are objected to because of the following informalities:

Claim 25, the term of "computer readable storage medium" is not defined in the present specification.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7 and 16-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Ptacek et al. [US. 2005/0005017]. The provisional application 60/484,873 has been considered and the following rejection is fully supported by the provisional application.

**As to claims 1, 18 and 25,** Ptacek et al. teach a method of analyzing security events, comprising: receiving and processing a stream of security events (page 1, 0011), including grouping the security events into network sessions (figure 1), each session having an identified source and destination (figure 3, 318, 322); displaying a graph representing devices (figure 1) in a network, the devices including security devices (firewall) and non-security devices (disk array), the displayed graph including a plurality of individual device symbols and a plurality of group device symbols (figure 1, 114-1, 114-2, 114-3...), each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; and displaying in conjunction with the graph security incident information, including with respect to a group device symbol an incident volume indicator (figure 1, 114-1, 114-2, 114-3...) that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol (page 3, 0032-0038).

**As to claims 2, 19 and 26,** Ptacek et al. teach upon user selection of a group device symbol for a group of non-security devices, displaying a second level graph representing the non-security devices in the group and the security devices in association with the group (the second level graph is disclosed at figure 2), the displayed second level graph including a plurality of non-security device symbols (figure 2, database of signatures) and a plurality of security device symbols (figure 2, firewall 1-3), each non-security device symbol

Art Unit: 2179

representing one non-security device in the group and each security device symbol representing one security device in the group; and displaying in conjunction with the second level graph security incident information, including with respect to a non-security device symbol an incident volume indicator (figure 2, firewall 1, firewall 2, firewall 3) that indicates a number of network sessions whose source or destination is at the non-security device (figure 3, 318, 322).

**As to claims 3, 20 and 27**, Ptacek et al. teach upon user command with respect to a user specified device symbol in the displayed graph, displaying data representing network sessions whose source or destination is at a device corresponding to the user specified device symbol (page 4, 0060, 0061).

**As to claims 4, 21 and 28**, Ptacek et al. teach in response to one or more user commands, selecting a network session from the displayed data, and defining a drop rule that comprises a set of network conditions corresponding to the selected network session; wherein the processing of security events includes filtering out network sessions that satisfy the defined drop rule (0046-0048).

**As to claims 5, 22 and 29**, Ptacek et al. teach source and destination identifying information, event type information indicating one or more types of incidents corresponding to the network sessions, and security device information indicating one or more security devices that report security events in association with the network sessions (0010-0011).

**As to claims 6, 23 and 30**, Ptacek et al. teach the processing of security events including identifying groups of network sessions that together satisfy a security incident identification rule in a group of predefined security incident identification rules, and identifying as rule firing network sessions each of the network sessions that is a member of any identified group of network sessions; wherein each incident volume indicator indicates a number of rule firing network sessions whose source or destination is at a device corresponding to the device symbol (0046-0068 and 0099).

**As to claims 7, 24 and 31**, Ptacek et al. teach the processing of security events including excluding from the rule firing network sessions any network session that satisfies any drop rule in a set of drop rules, each drop rule defining a respective set of conditions (0098-0099).

**As to claims 16 and 17**, Ptacek et al. teach a method of analyzing security events, comprising: receiving and processing security events (page 1, 0011), including grouping the security events into network sessions (figure 1), each session having an identified source and destination (figure 3, 318, 322); applying a plurality of predefined security event correlation rules to the plurality of network sessions in association with the processed security events (0046-0048); for each of a subset of the predefined security event correlation rules, identifying network sessions from the plurality of network sessions in association with the processed security events, if any, that satisfy the rule (0008-0010);

Art Unit: 2179

displaying a graph representing devices (figure 1) in a network, the devices including security devices (firewall) and non-security devices (disk array), the displayed graph including a plurality of individual device symbols and a plurality of group device symbols (figure 1, 114-1, 114-2, 114-3...), each individual device symbol representing a security device of the network and each group device symbol representing a group of non-security devices of the network; and displaying in conjunction with the graph security incident information, including with respect to a group device symbol an incident volume indicator (figure 1, 114-1, 114-2, 114-3...) that indicates a number of network sessions whose source or destination is at any member of a group of non-security devices corresponding to the group device symbol (page 3, 0032-0038).

### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mylinh Tran. The examiner can normally be reached on Mon - Thu from 7:00AM to 3:00PM at 571-272-4141.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Weilun Lo, can be reached at 571-272-4847.

The fax phone numbers for the organization where this application or proceeding is assigned are as follows:

571-273-8300

Art Unit: 2179

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mylinh Tran

Art Unit 2179

  
**WEILUN LO**  
SUPERVISORY PATENT EXAMINER